ネットコミュニケーション研究部門活動報告

武藏 泰雄[†] 久保田 真一郎[†] 杉谷 賢一[†]

[†]熊本大学総合情報基盤センター・ネットコミュニケーション研究部

概要: 平成 21 年度におけるネットコミュニケーション研究部門における研究報告事項について無線 LAN 関係と情報セキュリティ関係の二つがある。前者は、実環境における無線 LAN アクセスポイントからの受信信号強度を用いた位置推定手法の検討であり、また、後者は、DNS 通信監視によるホスト探索検知技術および SSH 辞書攻撃検知技術の開発研究である。

1. 背景

大学のキャンパスネットワークにおいて、不正に設置された、または野良 AP と呼ばれる無線 LAN アクセスポイント(AP)を放置することは、情報セキュリティまたはネットワークセキュリティの観点から、例えば盗聴や乗っ取りなどによる情報漏洩につながる恐れがあり、非常に危険であると言える。従ってその位置を特定する必要がある。

一方で、大学のサーバは常に SSH 辞書攻撃に晒されており、これを検知する技術が必要であるが、現時点で実装されているセキュリティアプライアンスでは、困難であり、サーバ群がどのように攻撃されるかを検知することも実際のところ困難であることが多い。更に、DNS サーバに対して、学内の IP アドレスに割り当てられたサーバのホスト名を連続的、逆引き名前解決を行うホスト探索(HS)攻撃も常に行われており、その検知は一般に難しい。

そこで、我々の研究部門においては、無線 LAN AP における受信信号強度に基づいた位置の特定に関する技術開発およびホスト探索攻撃や SSH 辞書攻撃検知技術の開発検討を行ったので報告したい。

2. 実環境における無線 LAN 受信信号強度を用いた位置推定手法の検討

熊本大学には，学内利用者用に約 450 個のアクセスポイントが各所に設置され、多くの場所でネットワークを利用できる環境にある．われわれはこれらの無線 LAN アクセスポイントから受信する受信信号強度を利用した位置推定技術の検討に近年取り組んでいる。平成 12 年 11 月に実施された九州情報通信連携推進協議会（KIAI=Kyushu Island Alliance of ICT）が行う事業の平成 21 年度実証実験に、現在利用を検討している推定技術を検証する実験計画を持ち込み、実験を行った。実験は、宮崎県美郷町で行われたが、この実験の副題が、「地理的条件不利地域における臨時的情報通信インフラ網構築実験」となり、不利地域における災害発生時の情報インフラを一時的に構築するための実証実験の一環にもなっていることを付記しておく。

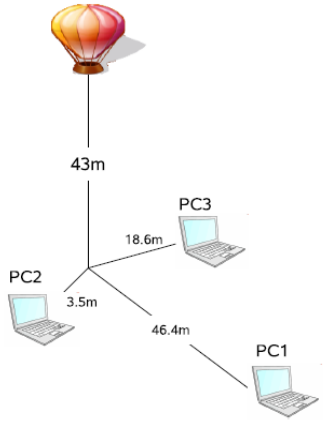

図 1 係留されていたバルーンの模式図

図 2 信号強度と距離の相関係数と時系列データによる分布

図1に実験装置を示す。図1のバルーンの部分に無線 LAN を設置し、地上では 3 台の PC で Network Stumbler を使用して無線 LAN通信を発生させ、信号強度の測定を行った。無線局間の距離 r と受信信号強度（$\Lambda(r)$）との関係式は、正規分布に従うと仮定し、下記の式(1)で表現されるとする。

$$p(P_r \mid r) = \frac{1}{\sqrt{2\pi\delta^2}} \exp\left(-\frac{(P_r - \Lambda(r))^2}{2\delta^2}\right) \qquad (1)$$

約４５時間測定で得られたデータをもとに距離 r を最尤推定法で求めた。まず時系列と受信強度を調査すると一様分布ではないことがわかったので、最尤度推定を行った結果、35.03m $\leq r \leq$ 52.77m (実測値は 43m)が得られた。誤差の範囲が±5.2m である。時系列のデータを分割して、信号強度と距離の相関係数を調査すると図 2 に示すように、時系列データによって相関係数が高い部分があり、良いデータが存在することがわかる。そこで、信号強度と距離の相関係数が高く、分散小さい、良いデータ同士は相関があるという仮説を立てて、推定を行った結果、39.65m $\leq r \leq$ 52.82m が得られ、推定精度が向上することが示された。これらの結果は、平成 22 年 3 月の情報処理学会インターネットと運用技術研究会(IOT08)で発表した[1]。

3. DNS 通信監視によるホスト探索攻撃および SSH 辞書攻撃の検知技術の開発

本大学では、プライマリドメイン名 DNS サーバに対する様々な DNS クライアントからの DNS 名前解決要求パケット(DNS クエリパケット略す)のキャプチャリングを行っており、毎日統計解析を行っている。HS 攻撃については、一日当たりデータセットについて、クエリキーワードの頻度や送信元 IP アドレスの頻度についてエントロピー解析を行えば、検出は可能である。しかしながら、HS 探索攻撃は高速に行われることが多く、できるだけ速やかに検知して、その攻撃を遮断しなければならない。また SSH 辞書攻撃も同様であるため、リアルタイムに検知する必要がある。SSH 攻撃を受けるサーバは一般にログへホストドメイン名を攻撃元の IP アドレスと同時に記録するため、DNS サーバに対して大量の DNS 名前解決要求する。そのためこれらの DNS クエリパケットを監視すれば、サーバが間接的であるが SSH 辞書攻撃を受けていることがリアルタイムにわかる。いずれにしても、これらの DNS クエリパケット通信における特徴は、DNS クエリパケット通信の時系列分布は一様分布であり、クエリキーワードが IP アドレス($\mathbf{IP}_i=[x_{i,j}]$)であり、ベクトルとして扱えることから、現在のパケットと直前のパケットの IP アドレスについてユークリッド距離 $\mathbf{d(IP_i, IP_{i-1})}$(式(2))を測定することが可能である。

$$d(IP_i, IP_{i-1}) = \sqrt{\sum^{4} (x_{i,j} - x_{i-1,j})^2} \quad (2)$$

HS 攻撃については、$\mathbf{d(IP_i, IP_{i-1})}$の頻度分布が、1.0-2.0 (連続的、狭い範囲で一様分布または指数分布)または 150.2-210.4 （正規分布）になることが、調査の結果わかった。また、SSH 辞書攻撃を受けたサーバからの DNS クエリパケットのクエリキーワードの IP アドレスは一定であるため、$\mathbf{d(IP_i, IP_{i-1})}$の頻度が常に 0 となる。

図 3 では、HS 攻撃のスコアの変化を示しおり、13 個のピークが観察される。また図 4 では、SSH 辞書攻撃に

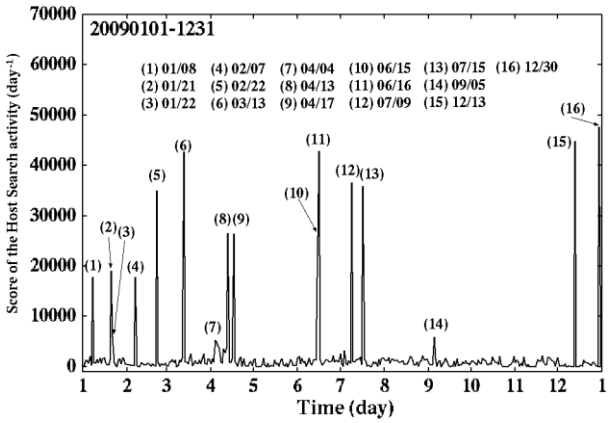

図 3 ホスト探索攻撃の検知スコア変化

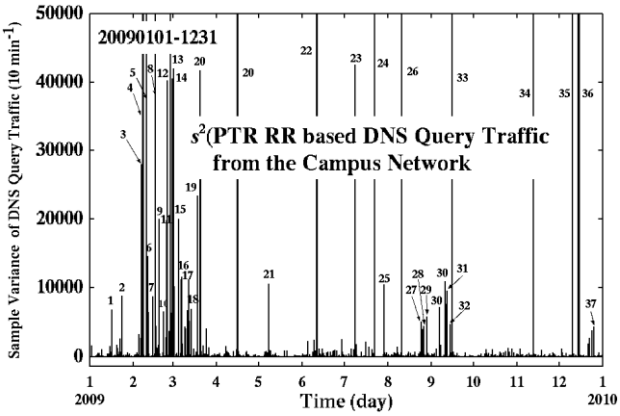

図 4 SSH 辞書攻撃の分散の変化

によって間接的に起こる DNS クエリパケット流量の分散の変化を示しており、37 個のピークが観察される[2]。

4. 今後の展開

以上の結果から、本大学のキャンパスネットワークは外部から多くの SSH 辞書攻撃を受けている可能性があること、またホスト探索攻撃も頻繁に行われていることがわかる。また、無線 LAN の位置推定手法についても、良いデータを正確に得るための技術が必要である。

謝辞

我々の研究はすべて総合情報基盤センターの設備を使って行われた。て熊本大学の教職員及び学生の皆様のご理解ご協力に厚く感謝申し上げます。

参考文献

[1] 川村諒, 副島慶人, 久保田真一郎, 古川誠一郎, 杉谷賢一:, 実環境における無線 LAN 受信信号強度を用いた位置推定手法の検討, インターネットと運用技術研究会(IOT08), Vol.2010-IOT-8 No.51, pp.1-4 (2010)

[2] Min Lei, Yasuo Musashi, Dennis Arturo Ludeña Romaña, Kazuya Takemori, Shinichiro Kubota, and Keinchi Sugitani: Detection of Host Search Activity in Domain Name Reverse Resolution Traffic, IPSJ Symposium Series (IOTS2009), Vol. 2009, No. 15, pp.91-94 (2009)